<u>In the Drawings</u>:

Amend FIGs. 3A and 4 as indicated in red on the enclosed copies of the drawings as filed.

<u>In the Specification</u>:

Replace the Specification as-filed with the enclosed substitute Specification. A copy of the Specification as-filed, marked up to indicate words being [deleted] or <u>inserted</u>, is also enclosed. No new matter is being introduced.

<u>In the Claims</u>:

For the Examiner's convenience, all of the pending claims as they will stand after this amendment are reproduced below.

1   1.   (Amended) A system for maintaining security in a distributed computing environment,

2   comprising:

3   (1) a policy manager, coupled to a network, including

4   a database for storing a security policy including a plurality of rules; and

5   a policy distributor, coupled to the database, for distributing the rules through the

6   network;

7   (2) a security engine, coupled to the network, for storing a set of rules received through the

8   network from the policy distributor and for enforcing the rules with respect to an application; and

9   (3) an application, coupled to the security engine.

1   2.   (Amended) The system of claim 1, wherein the rules are stored separate from the

2   application.

1   3.   (Amended) The system of claim 1, wherein the security engine further comprises:

2   an engine for, based on the rules, evaluating a request to access the application; and

3   an application programming interface (API) for enabling the application and the engine to

4   communicate.

1   4.   The system of claim 3, wherein the security engine further comprises: a plug-in application

2   programming interface (plug-in API) for extending capabilities of the security engine.

1   5.   The system of claim 1, further comprising: location means for enabling components in the

2   system to locate each other through the network.

1   6.   The system of claim 1, wherein the policy manager and the policy distributor are hosted on

2   a first server, the security engine and the application are hosted on a second server, and the first and

3   second servers are communicatively coupled to each other through the network.

1   7.   A system for maintaining security for an application in a distributed computing

2   environment, comprising:

3   an engine, coupled to a network, for storing a set of rules received through the network

4   from a centralized location and for enforcing the rules;

5   ·   an interface coupled to the engine; and

6   an application, coupled to the interface to enable the application to communicate with the

7   engine.

1   8.   (Amended) The system of claim 7, wherein the engine stores the rules separate from the

2   application.

1   9.   The system of claim 7, further comprising: a plug-in application programming interface

2   (plug-in API) for extending capabilities of the security engine.

1   10.   (Amended) A system for maintaining security in a distributed computing environment,

2   comprising:

3   (1) a policy manager, coupled to a network, including

4   a database for storing a security policy including a plurality of rules; and

5   a policy distributor for distributing the rules through the network;

6   (2) a plurality of security engines, each coupled to the network, for receiving a set of rules

7   through the network from the policy distributor, storing the set of rules, and enforcing the set of

8   rules; and

9   (3) a plurality of applications, each application being coupled to a respective security

10   engine, each security engine being able to enforce a set of rules for its respective application.

1   11.   (Amended) The system of claim 10, wherein the security engines store the rules separate

2   from each application.

1   12.   The system of claim 10, wherein each security engine further comprises:

2   an engine for, based on a set of rules, evaluating a request to access a particular application;

3   and

4   an application programming interface (API) for enabling a respective application to

5   communicate with a respective engine.

1   13.   The system of claim 12, wherein each security engine further comprises: a plug-in

2   application programming interface (plug-in API) for extending capabilities of the security engine.

1   14.   The system of claim 10, further comprising: location means for enabling components in the

2   system to locate each other through the network.

1 15. The system of claim 10, wherein the policy manager and the policy distributor are hosted on
2 a policy server, the plurality of security engines and the plurality of applications are hosted on at
3 least one separate server, and the policy server is communicatively coupled through the network to
4 the separate server.

1 16. A system for maintaining security for a plurality of applications in a distributed computing
2 environment, comprising:
3   an engine, coupled to a network, for storing a set of rules received through the network
4 from a centralized location, and for enforcing the rules;
5   a plurality of interfaces coupled to the engine; and
6   a plurality of applications, each application being coupled to a respective interface to enable
7 the application to communicate with the engine through its respective interface, wherein the
8 engines enforcing the rules for the application.

1 17. The system of claim 16, wherein the rules are separate from each application.

1 18. The system of claim 17, further comprising: a plug-in application programming interface
2 (plug-in API) for extending capabilities of the engine.

Cancel claims 19 - 33

Add the following new claims 34 - 35

1 34. A system for maintaining security in a distributed computing environment, comprising:

2   a policy manager including a policy database for storing a security policy having a plurality

3 of rules;

4   zero or more security engines for storing and enforcing a set of rules with respect to an

5 application, said policy manager and said zero or more security engines residing on a single server;

6 and

7   an application, coupled to the zero or more security engines;

8 wherein updates to security policies residing on other servers may be synchronized through

9 database replication.

1 35. A system for maintaining security in a distributed computing environment, comprising:

2   a policy manager including a policy database for storing a security policy having a plurality

3 of rules;

4   zero or more security engines for storing and enforcing a set of rules with respect to an

5 application, said policy manager and said zero or more security engines residing on a central

6 server; and

7   an application, coupled to the zero or more security engines;

8 wherein other servers storing local security policies may, in response to an authorization request,

9 synchronize local security policy updates with the central server.